

# Проблемы скрытой передачи информации

Михаил Калинин, генеральный директор компании StarForce Technologies



В поисках ответа на вопрос: "Какие есть проблемы в сфере скрытой передачи информации?" – хотелось бы обратить внимание на наиболее популярные способы скрытой передачи информации – сокрытие данных в массиве цифрового изображения или файла, а также использование специальных протоколов (туннелирование).

**ПРИ** существующем сегодня огромном количестве серверов и каналов передачи данных скрытно передать ту или иную информацию не составляет труда. Однако на деле все оказывается не так уж и просто. При переходе к практической стороне дела встает вопрос: "Каким образом можно утаить сам факт передачи информации?" В это же время многие сотрудники служб безопасности озабочены вопросом, как выявить скрытую передачу данных. Согласитесь, спецслужбы просто так думать над этим вопросом не будут. А значит, существует проблема и... ее решение.

## Стеганография: от невидимых чернил до микроточек

В настоящее время, когда информация играет важнейшую роль в вопросах конкурентной борьбы, в дело вступают технологии промышленного шпионажа. Теперь руководители и специалисты по информационной безопасности размышляют не только над тем, как наиболее надежно сохранить коммерчески важную информацию, но и о том, как эту информацию незаметно передать. В то же время нужно следить за тем, чтобы коммерчески важная информация не ушла из компании к конкурентам.

Само явление скрытия передачи информации известно

примерно с V в. до нашей эры и называется стеганографией. Всем нам еще с детства помнятся невидимые чернила или письма, написанные молоком. Во время Второй мировой войны германские спецслужбы могли передавать секретные данные в обычных письмах или открытках. Чтобы достичь этого, на место обычных знаков препинания клеивались микроточки, представляющие собой крошечные фотографии. Такие микроточки могли содержать тексты, чертежи, фотографии. Со временем методы стеганографии менялись, а с развитием информационных технологий появилось новое направление в сфере защиты информации – компьютерная стеганография. Под этим явлением подразумевается скрытие информации в текстовых, графических или видеофайлах с использованием специальных программ.

## Способы скрытой передачи информации

Наиболее простым способом скрытия информации является встраивание данных в плоскость изображения. При этом внедряемая скрытая информация не должна влиять на качество графики. Осуществляется этот способ с помощью встраивания в файл-контейнер (например, рисунок в формате jpg) определенного сообщения, при этом используется специальный стегоключ. Этот секретный ключ нужен не только для встраивания информации в файл, но и для последующего чтения данных.

В других ситуациях данные скрывают в неиспользуемых областях форматов файлов. Удобство этого способа заключается в том, что в качестве контейнера могут служить практически любые файлы: аудио, видео, картинки и т.п. Внесение изменений в них не приводит к заметным искажениям исходного файла. В качестве примера можно привести известный вирус WIN95.CIH. Этот вирус встраивается в исполняемый файл \*.exe, используя незаполненные секции формата PE (Portable Executable). Как известно, \*.exe может содержать в себе не только код приложения, но и многочисленные дополнительные данные (например, пиктограммы, служебные данные и информацию о функциях), которые хранятся в отдельных секциях формата PE. Если же данные не заполняют секцию полностью, то они не используются, и в результате остается достаточно много места. Примерно такая же технология используется в других случаях. Недостаток этого способа в том, что встраиваемые данные и данные файла-контейнера существуют отдельно друг от друга, соответственно степень защищенности может понизиться.

Главным требованием при передаче информации является то, что измененный файл не должен для стороннего наблюдателя отличаться от исходного контейнера. Добиться такого эффекта возможно с помощью использования специализированных программ, например StegoMagic. Известны и другие аналоги такого программного обеспечения, позволяющие скрыть информацию в bmp, dib, wav и html-файлах (S-Tools, Steganos for Wins). Зачастую эти программы имеют простой пользовательский интерфейс и очень удобны в использовании даже для неподготовленного человека.

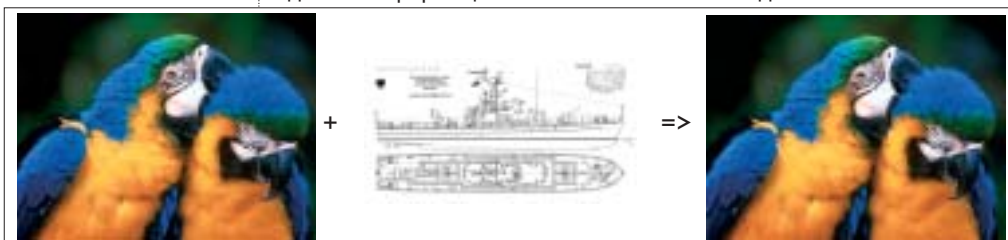


Рисунок. Встраивание данных в плоскость изображения

Тем не менее описанные выше способы сокрытия информации не всегда применимы при жестком администрировании ее передачи. Администратору далеко не всегда нужно просматривать файл в поисках встроенной информации, достаточно учитывать, на какие адреса отправляются и с каких узлов принимаются файлы. Ведь если от финансового директора в адрес конкурирующей фирмы будут регулярно уходить картинки с йоркширскими терьерами, то это повод задуматься!

Достаточно часто для скрытой передачи информации идут другим путем, используя скрытые каналы связи. Каналы такого типа создаются специальными программами для обхода firewall и корпоративных систем фильтрации.

Проблема использования туннелирования состоит в том, что эти же скрытые каналы могут использовать ботнеты (сети зараженных компьютеров). Решением проблемы может быть установка сетевых устройств, лучше "понимающих" новый протокол. Еще одним способом

закрыть этот вопрос является отслеживание трафика: если много так называемого "левого" трафика, то возможно заблокировать сервер, на который уходит большое количество мегабайт. Кроме того, нельзя пренебрегать элементарными средствами предосторожности: следить за теми, кто имеет доступ к важной информации, контролировать ее пересылку и возможность копирования.

Для защиты от скрытой передачи информации надо стремиться анализировать и контролировать не столько способы передачи информации, сколько доступ к самой информации и ее модификацию. Действительно, невозможно найти то, что неизвестно где искать. Просто пытаться выявить скрытую неизвестным способом и в неизвестном файле информацию практически невозможно. Однако если добавить к этому возможность контролировать доступ к файлу и работу программ, которые использовались для его разработки, то эта задача становится вполне решаемой.

В целом можно выделить два подхода. Во-первых, мож-

но делать документы неотделимыми от программ их просмотра, которые, в свою очередь, привязываются к компьютеру. В этом случае программа просмотра активируется на конкретных компьютерах (например, в бухгалтерии), а документы защищаются таким образом, что их можно просмотреть только на данных копиях программ. Второй подход носит название поведенческого анализа и используется различными производителями. В этом случае на компьютеры сотрудников устанавливаются специальные программные модули, которые блокируют доступ к файлам любых программ, кроме разрешенных. В этом случае уже невозможно, например, присоединить документ к электронному письму или запустить программу, которая спрячет его внутри безобидной картинки.

В общем, как обычно, проблемы лучше предотвратить, чем потом лечить. ●

Ваше мнение и вопросы  
присылайте по адресу  
[infosec@groteck.ru](mailto:infosec@groteck.ru)

В августе 2006 г. миру была представлена программа для создания секретных каналов передачи данных – VoodooNet. Эта программа позволяла использовать для передачи пакетов шестую версию протокола управления сообщениями Internet (IPv6). В настоящее время мировое сообщество работает над созданием единого протокола, по примеру распространенного в азиатских странах.



**Пензенский филиал  
Федерального государственного  
унитарного предприятия  
"Научно-технический центр "Атлас"  
(ПФ ФГУП "НТЦ "Атлас")**

**Комплексное решение проблем  
обеспечения информационной безопасности,  
в том числе с использованием криптографии.  
Для выполнения всего комплекса задач  
ПФ ФГУП "НТЦ "Атлас" обладает необходимыми  
лицензиями и аккредитациями ФСБ России,  
ФСТЭК России, Министерства обороны РФ.**

440026, г. Пенза, ул. Советская, дом 9  
Тел.: (8412) 56-3916, 56-3397. Факс: (8412) 56-2371  
E-mail: [atlas@sura.ru](mailto:atlas@sura.ru), <http://www.atlas.sura.ru>